Block-Serial Finite Field Multipliers

Abstract

Finite field elements from the field GF(2^k) are represented as polynomials with binary valued coefficients. As such, multiplication in the field is defined modulo an irreducible polynomial of degree k-1. One of the multiplicands is treated in blocks of polynomials of degree n-1 so that the multiplier operates over T cycles where k = nT. If k is not a composite number to start with, higher order terms are added, so that multipliers are now constructable even when k is prime. Since n < k, the construction of the needed multiplier circuits are much simpler. Designers are now provided with an opportunity of easily trading off circuit speed for circuit complexity in an orderly and structured fashion.